The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
5/26/2016

SUBJECT:
Multiple Vulnerabilities in PHP Could Allow For Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in PHP, the most severe of which could allow an attacker to execute arbitrary code, with failed exploit attempts potentially leading to denial of service conditions. PHP is a programming language originally designed for use in web-based applications with HTML content. PHP supports a wide variety of platforms and is used by numerous web-based software applications. Successfully exploiting these issues could allow remote attackers to execute arbitrary code in the context of the affected application.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild. There is known proof-of-concept code for these vulnerabilities.

SYSTEMS AFFECTED:
- PHP 5 prior to 5.5.36
- PHP 7 prior to 7.0.7

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
PHP has released updates that address multiple vulnerabilities, the most severe of which could allow for arbitrary code execution. These vulnerabilities include:

Prior to 5.5.36
- Fixed bug #71331 (Uninitialized pointer in phar_make_dirstream()).
- Fixed bug #72114 (Integer underflow / arbitrary null write in fread/gzread).
- Fixed bug #72135 (Integer Overflow in php_html_entities).

- Fixed bug #72227 (imagescale out-of-bounds read).
- Fixed bug #72241 (get_icu_value_internal out-of-bounds read).

Prior to 7.0.7

- Add compiler option to disable special case function calls.
- Added socket_export_stream() function for getting a stream compatible resource from a socket resource.
- Fixed bug #68658 (Define CURLE_SSL_CACERT_BADFILE).
- Fixed bug #68849 (bindValue is not using the right data type).
- Fixed bug #71062 (pg_convert() doesn't accept ISO 8601 for datatype timestamp).
- Fixed bug #71600 (oci_fetch_all segfaults when selecting more than eight columns).
- Fixed bug #71737 (Memory leak in closure with parameter named $this).
- Fixed bug #71972 (Cyclic references causing session_start(): Failed to decode session object).
- Fixed bug #72014 (Including a file with anonymous classes multiple times leads to fatal error).
- Fixed bug #72028 (pg_query_params(): NULL converts to empty string).
- Fixed bug #72031 (array_column() against an array of objects discards all values matching null).
- Fixed bug #72038 (Function calls with values to a by-ref parameter don't always throw a notice).
- Fixed bug #72051 (The reference in CallbackFilterIterator doesn't work as expected).
- Fixed bug #72057 (PHP Hangs when using custom error handler and typehint).
- Fixed bug #72059 (?? is not allowed on constant expressions).
- Fixed bug #72069 (Behavior \JsonSerializable different from json_encode).
- Fixed bug #72075 (Referencing socket resources breaks stream_select).
- Fixed bug #72100 (implode() inserts garbage into resulting string when joins very big integer).
- Fixed bug #72101 (crash on complex code).
- Fixed bug #72133 (php_posix_group_to_array crashes if gr_passwd is NULL).
- Fixed bug #72151 (mysqli_fetch_object changed behaviour).
- Fixed bug #72154 (pcntl_wait/pcntl_waitpid array internal structure overwrite).
- Fixed bug #72157 (use-after-free caused by dba_open).
- Fixed bug #72159 (Imported Class Overrides Local Class Name).
- Fixed bug #72162 (use-after-free - error_reporting).
- Fixed bug #72164 (Null Pointer Dereference - mb_ereg_replace).
- Fixed bug #72165 (Null pointer dereference - openssl_csr_new).
- Fixed bug #72174 (ReflectionProperty#getValue() causes __isset call).
- Fixed bug #72227 (imagescale out-of-bounds read).
- Fixed bug #72241 (get_icu_value_internal out-of-bounds read).

Successfully exploiting these issues could allow remote attackers to execute arbitrary code in the context of the affected application.

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade to the latest version of PHP immediately, after appropriate testing.
- Apply the principle of Least Privilege to all systems and services..
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.

- Limit user account privileges to only those required.

REFERENCES:

NOTE: Visiting these links may trigger an IDS signature match for a Possible Encrypted Webshell Download. This is a false positive alert that is matching content on the pages below.

PHP:
http://php.net/ChangeLog-5.php#5.5.36
http://php.net/ChangeLog-7.php#7.0.7